

Nessus Vulnerability Scanning Project

Table of Contents

1. Project Overview
2. What is Nessus?
3. Prerequisites
4. Installation Guide
5. Initial Configuration
6. Performing Vulnerability Scans
7. Analyzing Scan Results
8. Critical Findings to Look For
9. Remediation Strategies
10. Security Best Practices
11. Advantages and Disadvantages
12. Real-World Use Cases
13. Conclusions and Recommendations
14. Additional Resources

Project Overview

Purpose

This project demonstrates the complete workflow of using Nessus vulnerability scanner to identify, analyze, and remediate security vulnerabilities in a network environment using Kali Linux on Oracle VirtualBox.

Learning Objectives

- Understand vulnerability assessment fundamentals
- Install and configure Nessus Essentials
- Perform comprehensive vulnerability scans
- Analyze and prioritize security findings

- Develop remediation strategies
- Apply security best practices

Environment

- **Host OS:** Windows/macOS/Linux
- **Virtualization:** Oracle VirtualBox
- **Guest OS:** Kali Linux (Latest version)
- **Scanner:** Nessus Essentials (Free version)
- **Target:** Metasploitable 2/3 or other vulnerable VMs

What is Nessus?

Definition

Nessus is a comprehensive vulnerability assessment solution developed by Tenable that identifies security weaknesses, configuration issues, malware, and policy violations across networks, systems, and applications.

Key Features

- **60,000+ vulnerability checks:** Extensive plugin library
- **Configuration auditing:** CIS benchmarks, PCI-DSS compliance
- **Malware detection:** Identifies suspicious processes
- **Credentialed scanning:** Deep system analysis
- **Web application scanning:** OWASP Top 10 vulnerabilities
- **Cloud infrastructure scanning:** AWS, Azure, GCP support

How It Works

1. **Discovery Phase:** Identifies live hosts and open ports
2. **Vulnerability Detection:** Tests for known vulnerabilities
3. **Analysis:** Assigns severity ratings (Critical, High, Medium, Low, Info)
4. **Reporting:** Generates detailed reports with remediation guidance

Prerequisites

Hardware Requirements

- **RAM:** Minimum 4GB (8GB recommended)
- **Storage:** 20GB free space
- **CPU:** Dual-core processor (Quad-core recommended)
- **Network:** Active internet connection

Software Requirements

- Oracle VirtualBox (latest version)
- Kali Linux ISO (latest version)
- Target vulnerable VM (Metasploitable 2 recommended)

Knowledge Requirements

- Basic Linux command-line skills
- Understanding of networking concepts (IP, TCP/IP, ports)
- Familiarity with cybersecurity terminology

Installation Guide

Step 1: Download Nessus Essentials

1. Navigate to: <https://www.tenable.com/products/nessus/nessus-essentials>
2. Click "**Register for Nessus Essentials**"
3. Fill out the registration form with valid email
4. Select "**Nessus-#.##.#-debian6_amd64.deb**" for Kali Linux
5. Save the activation code sent to your email

Step 2: Install Nessus on Kali Linux

Open a terminal and execute the following commands:

```
bash
```

Update system packages

```
sudo apt update && sudo apt upgrade -y
```

Navigate to the Downloads directory

```
cd ~/Downloads
```

Install the Nessus package

```
sudo dpkg -i Nessus-*.deb
```

Start Nessus service

```
sudo systemctl start nessusd
```

Enable Nessus to start on boot

```
sudo systemctl enable nessusd
```

Check service status

```
sudo systemctl status nessusd
```

```

Session Actions Edit View Help
└─(bjnetwork㉿bjnetwork)-[~]
$ ls Downloads
'Malware analysis PowerRun_x64.exe Malicious activity _ ANY.RUN - Malware Sandbox Online-1.pdf'
'Malware analysis PowerRun_x64.exe Malicious activity _ ANY.RUN - Malware Sandbox Online-1.pdf.zip'
'Malware analysis PowerRun_x64.exe Malicious activity _ ANY.RUN - Malware Sandbox Online.pdf'
Nessus-10.11.1-debian10_amd64.deb
pushpins.csv

└─(bjnetwork㉿bjnetwork)-[~]
$ sudo systemctl start nessusd
[sudo] password for bjnetwork:

└─(bjnetwork㉿bjnetwork)-[~]
$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
    Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
    Active: active (running) since Thu 2026-01-15 21:40:40 EST; 16s ago
      Invocation: 6bfaf49e3673455da09ff40967ef3eb5
        Main PID: 15305 (nessus-service)
          Tasks: 16 (limit: 4657)
        Memory: 2.2G (peak: 2.3G)
          CPU: 24.977s
        CGroup: /system.slice/nessusd.service
                └─15305 /opt/nessus/sbin/nessus-service -q
                  ├─15307 nessusd -q

Jan 15 21:40:40 bjnetwork systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Jan 15 21:40:40 bjnetwork nessus-service[15305]: nessus-service [15305][INFO] : Nessus 19.16.1 [buil
└─(bjnetwork㉿bjnetwork)-[~]
$ █

```

Step 3: Access Nessus Web Interface

bash

Nessus runs on port 8834

Open a web browser and navigate to:

<https://localhost:8834>

Initial Configuration

Step 1: Welcome and Setup

1. Click "Nessus Essentials."
2. Enter the activation code from your email
3. Create admin username and password (use strong credentials)
4. Click "Continue."

Step 2: Plugin Download

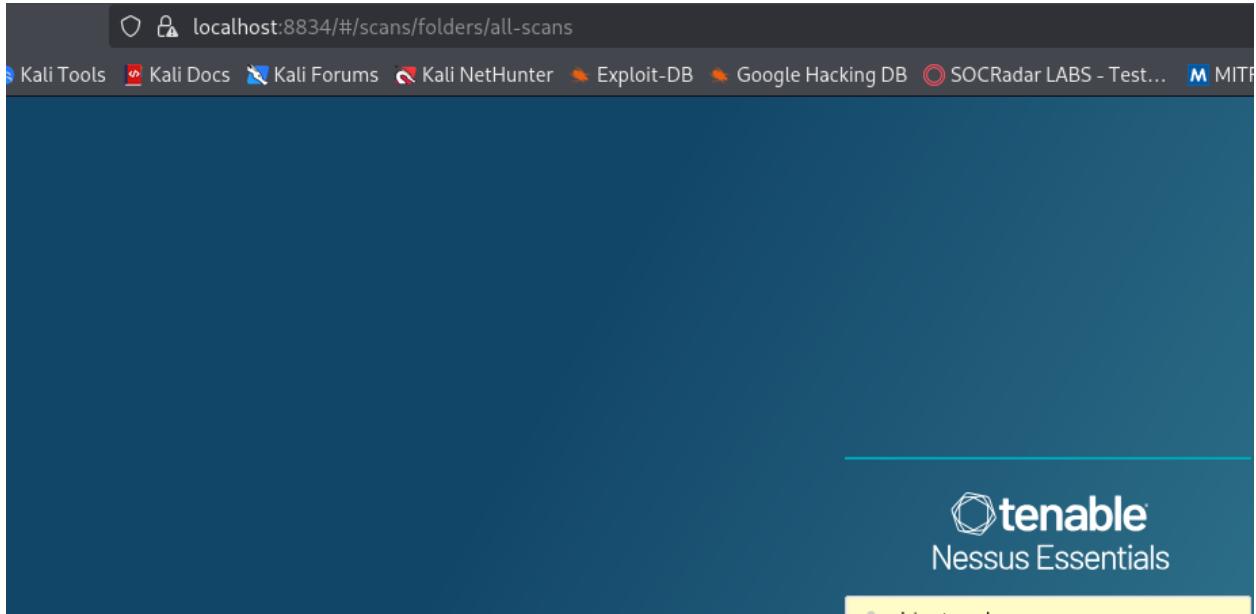
Wait time: 15-30 minutes for initial plugin compilation

bash

Monitor plugin compilation progress in terminal

```
sudo tail -f /opt/nessus/var/nessus/logs/nessusd.messages
```

Step 3: Log in to Nessus



- Navigate to <https://localhost:8834>
- Enter your admin credentials
- You should see the main Nessus dashboard

Performing Vulnerability Scans

Scan Types Overview

Scan Type	Purpose	Credentials Required	Duration
Basic Network Scan	Quick vulnerability assessment	No	5-15 min
Advanced Scan	Customizable with specific plugins	Optional	10-30 min
Credentialed Scan	Deep system analysis	Yes	20-60 min
Web Application Scan	OWASP vulnerabilities	No	15-45 min
Malware Scan	Detect malicious processes	Yes	10-30 min

Step 1: Create a New Scan

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'FOLDERS' containing 'My Scans' (marked with a '1'), 'All Scans', and 'Trash'. Below that is 'RESOURCES' with 'Policies' and 'Plugin Rules'. At the bottom left is a 'Tenable News' section. The main content area is titled 'Scan Templates' with a 'Back to Scans' link. It has tabs for 'Scanner' and 'DISCOVERY'. Under 'DISCOVERY', there are two cards: 'Host Discovery' (a simple scan to discover live hosts and open ports) and 'Ping-Only Discovery' (a simple scan to discover live hosts with minimal network traffic). Under 'VULNERABILITIES', there are ten cards arranged in two rows of five: 'Basic Network Scan' (a full system scan suitable for any host), 'Credential Validation' (verifies host credential pairs for Windows & Unix), 'Advanced Scan' (configures a scan without recommendations), 'Advanced Dynamic Scan' (configures a dynamic plugin scan without recommendations), 'Malware Scan' (scans for malware on Windows and Unix systems); the second row includes 'Web Application Tests' (scans for published and unknown web vulnerabilities), 'Credentialed Patch Audit' (authenticates hosts and enumerates missing updates), 'Active Directory Starter Scan' (looks for misconfigurations in Active Directory), 'Find AI' (AI, LLM, ML related detections and vulnerabilities), and 'Cryptographic Inventory' (probes network protocols to identify cryptography).

1. Click the "New Scan" button
2. Select "Basic Network Scan" for beginners
3. Configure scan settings:
 - o **Name:** "Initial Metasploitable Scan."
 - o **Description:** "First vulnerability assessment."
 - o **Folder:** My Scans
 - o **Targets:** 192.168.56.101 (your target VM IP)

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

General

Schedule

Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: Initial Metasploitable Scan

Description: First Vulnerability Assessment

Folder: My Scans

Targets: 10.0.2.3 10.0.0.105 halisans.com binetworksolution.xyz

Upload Targets Add File

Step 2: Configure Scan Settings (Advanced)

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

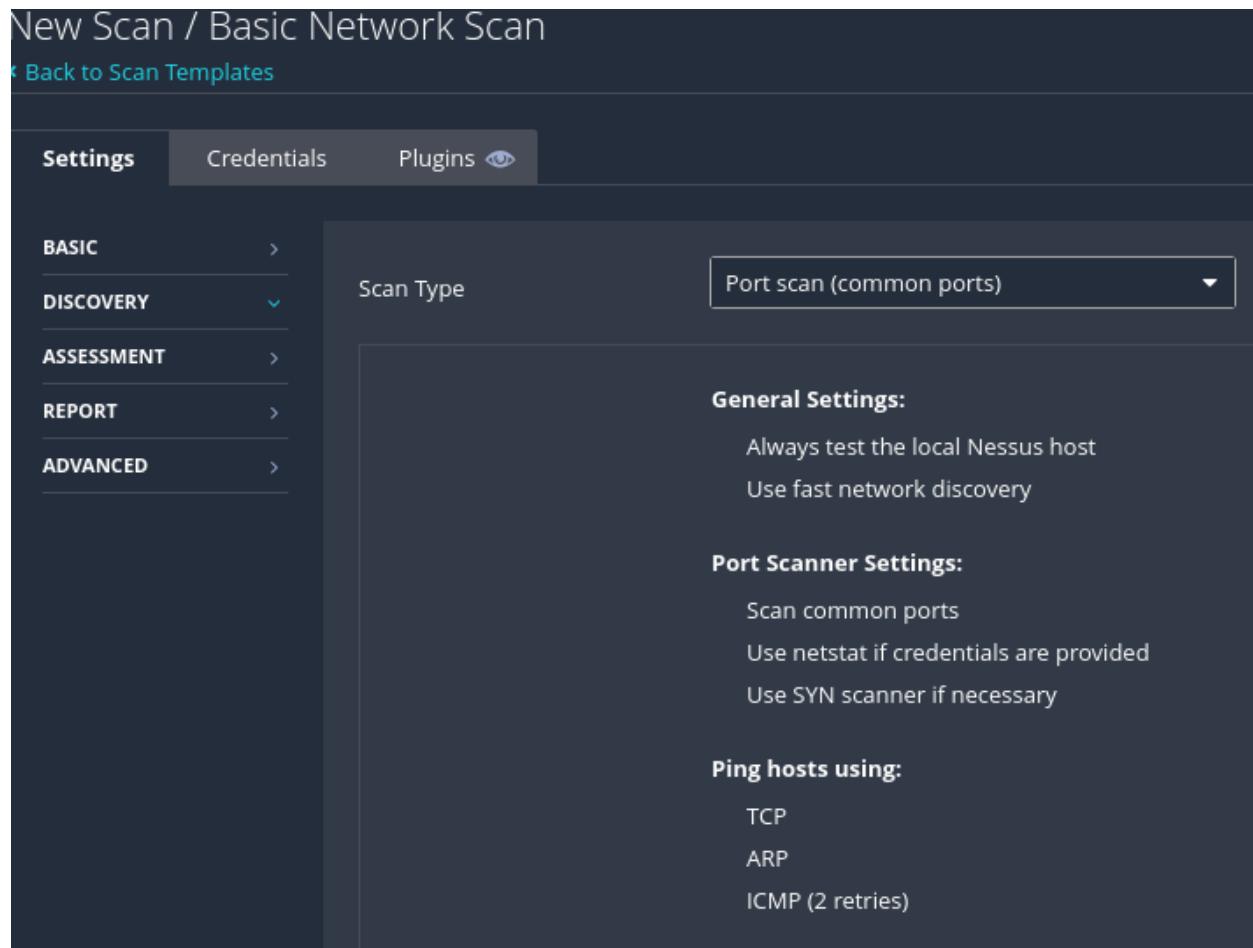
BASIC >
DISCOVERY <
ASSESSMENT >
REPORT >
ADVANCED >

Scan Type: Port scan (common ports)

General Settings:
Always test the local Nessus host
Use fast network discovery

Port Scanner Settings:
Scan common ports
Use netstat if credentials are provided
Use SYN scanner if necessary

Ping hosts using:
TCP
ARP
ICMP (2 retries)



Discovery Settings

Port Scanning:

- Port scan range: default (1-65535)
- Network discovery: Enabled

Assessment Settings

- General: Thorough tests
- Brute Force: Disabled (for initial scan)
- Web Applications: Enabled
- Malware: Enabled

Report Settings

- Output: HTML, PDF, CSV

- Processing: Enabled

Step 3: Launch the Scan

My Scans			
Scan Type	Schedule	Last Scanned	Import
Name	Vulnerability	On Demand	New Folder
Initial Metasploitable Scan		Today at 6:22 PM	

1. Click "**Save**" to save scan configuration
2. Click "**Launch**" to start scanning
3. Monitor progress in real-time

bash

Find target VM IP address

On target machine, run:

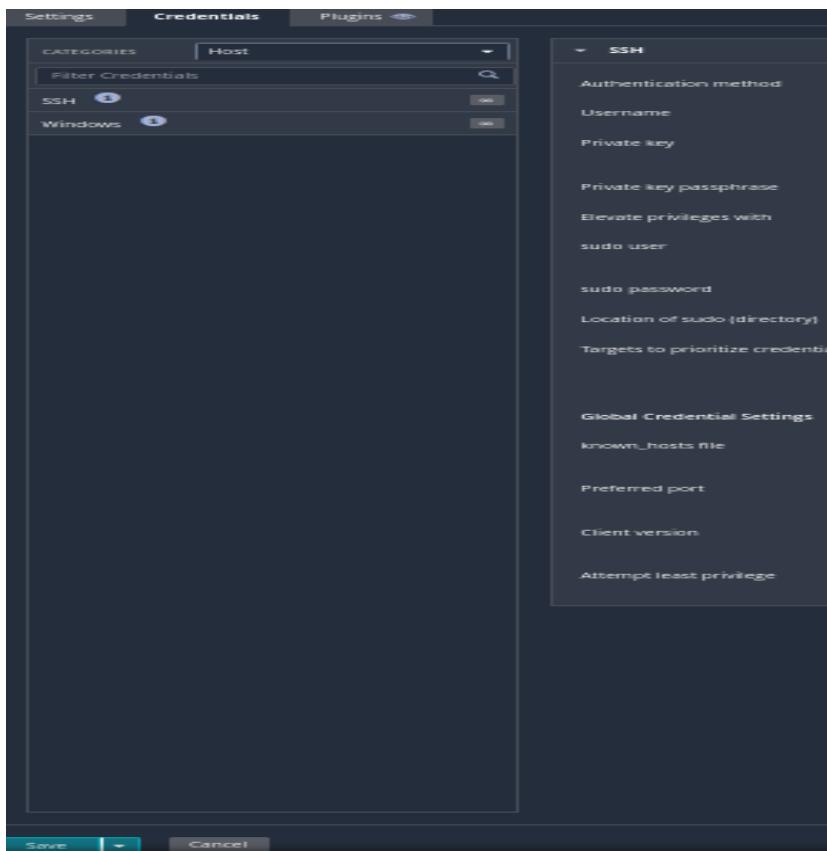
ifconfig

or

ip addr show

Step 4: Performing a Credentialed Scan

For deeper analysis, configure credentials:



1. Go to scan settings → "Credentials" tab
2. Select "SSH" for Linux targets
3. Add credentials:
 - o **Username:** msfadmin
 - o **Password:** msfadmin
 - o **Privilege Escalation:** sudo
4. Save and launch scan

Analyzing Scan Results

Understanding the Dashboard



The results page displays:

- **Vulnerabilities by Severity:** Color-coded graph
- **Host Summary:** Number of hosts scanned
- **Vulnerability Count:** Total findings

Severity Ratings Explained

Severity	Color	CVSS Score	Priority	Action Required
Critical	Purple	9.0-10.0	Immediate	Patch within 24 hours
High	Red	7.0-8.9	Urgent	Patch within 1 week
Medium	Orange	4.0-6.9	Moderate	Patch within 1 month
Low	Yellow	0.1-3.9	Minor	Schedule maintenance
Info	Blue	0.0	FYI	No action needed

Step 1: Review Vulnerabilities by Host

Vulnerabilities 73						
Filter ▾ Search Vulnerabilities				73 Vulnerabilities		
Sev	CVSS	VPR	EPSS	Name	Family	Count
Critical	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
Critical	10.0 *			UnrealIRCd Backdoor Detection	Backdoors	1
Critical	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
Critical	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
Critical	9.8			Bind Shell Backdoor Detection	Backdoors	1
Mixed	Apache Tomcat (Multiple Issues)	Web Servers	4

1. Click on the target IP address
2. Review all detected vulnerabilities
3. Sort by "Severity" (Critical → Low)

Step 2: Examine Individual Vulnerabilities

Plugin Details	
Severity:	Critical
ID:	201352
Version:	1.2
Type:	combined
Family:	General
Published:	July 3, 2024
Modified:	March 26, 2025
Risk Information	
Risk Factor: Critical	
CVSS v3.0 Base Score: 10.0	
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
CVSS v2.0 Base Score: 10.0	
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C	
Vulnerability Information	
CPE: cpe:/o:canonical:ubuntu_linux	

For each vulnerability, Nessus provides:

Essential Information

- **CVE ID:** Common Vulnerabilities and Exposures identifier
- **Description:** What the vulnerability is
- **Solution:** How to fix it
- **See Also:** Reference links
- **Plugin Output:** Specific evidence found
- **CVSS v3 Score:** Industry-standard severity rating
- **Exploitability:** Ease of exploitation

Example Vulnerability Analysis

Vulnerability: Samba Remote Code Execution

CVE: CVE-2017-7494

CVSS Score: 9.8 (Critical)

Risk Factor: Critical

Description:

Samba versions 3.5.0 through 4.6.4 contain a remote code execution vulnerability that allows attackers to upload a shared library to a writable share and execute arbitrary code.

Solution:

Upgrade to Samba version 4.6.4 or later

Exploit Available: Yes (Metasploit module exists)

CRITICAL Canonical Ubuntu Linux SEoL (8.04.x)

Description
According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution
Upgrade to a version of Canonical Ubuntu Linux that is currently supported.